Our Docket No.: 51876P371
Express Mail No.: EV339917613US

UTILITY APPLICATION FOR UNITED STATES PATENT

FOR

METHOD FOR AUTOMATICALLY ENTERING INTO SECURE COMMUNICATION MODE IN WIRELESS COMMUNICATION TERMINAL

Inventor(s):
Kyoung Ho Choi
Kil Ho Lee
Moon Seob Song
Joon Woo Lee

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
12400 Wilshire Boulevard, Seventh Floor
Los Angeles, California 90025
Telephone: (310) 207-3800

METHOD FOR AUTOMATICALLY ENTERING INTO SECURE COMMUNICATION MODE IN WIRELESS COMMUNICATION TERMINAL

Field of the Invention

The present invention relates to a wireless mobile communication terminal; and, more particularly, to a method for automatically entering into a secure communication mode to perform voice encryption between a transmission terminal and a reception terminal without changing or pre-setting a wireless mobile communication system, and a computer-readable recording medium for recording a program that can implement the method.

Description of Related Art

One of known secure communication technologies in a wireless mobile communication system is a Data Encryption Standard (DES), which encrypts data using a private key. In DES, more than 72×10^{15} private keys are used. Keys for each message are selected at random from the plenty of keys. Just as other private key encryption methods, both transmission and reception terminals should know and use the same private key. In the DES technology, 56 bits are used as a key in a 64-bit data block. This process can be performed in various modes, and it should go through 16 times of operations. DES was developed by IBM, and it is adopted as a Federal Standard in 1977. DES is in the American National Standards Institute

(ANSI) X3.92 and X3.106 Standard and the Federal Information Processing Standards (FIPS) 46 and 81.

The conventional secure communication system, however, has a shortcoming that it necessarily needs a voice communication security device, i.e., an encryption device, to secure voice communication. The voice communication security device is a system only for protecting voice communication from wiretapping.

Another conventional technology for secure voice communication is an Authentication Voice Privacy technology. In this technology, a particular message for attempting secured voice communication is transmitted from a transmission terminal to a base station, and the base station transmits a message for authentication to a reception terminal to perform secured voice communication.

However, this technology, too, has problems that a particular message for secured voice communication should be pre-set in the communication system. Since the base station knows that the communication channel is established for secured voice communication, the communication channel can become an object to be attacked.

Summary of the Invention

It is, therefore, an object of the present invention to provide a method for entering into a secure communication mode from a normal communication mode by forming part of a voice

signal communicated between a transmission terminal and a reception terminal as a token for attempting secured voice communication without changing the conventional establishment of a wireless mobile communication system, and a computer-readable recording medium for recording a program that implements the method. Other object(s) and advantage(s) of the present invention could be understood to those ordinarily skilled in the art from the accompanying drawings, detailed description of the invention and claims.

In accordance with an aspect of the present invention, there is provided a method for automatically entering into a secure communication mode in a wireless communication terminal, including the steps of: a) generating a token based on a data having the lowest frequency of generation among the voice data outputted from a vocoder of the wireless communication terminal; b) at a transmission terminal receiving a request for a secure communication from a user and transmitting the token to a reception terminal; and c) at the transmission terminal entering into a secure communication mode based on an acknowledge token transmitted from the reception terminal, and performing secure communication with the reception terminal.

In accordance with another aspect of the present invention, there is provided a computer-readable recording medium for recording a program that implements a method for automatically entering into a secure communication mode in a wireless communication terminal provided with a processor, including the steps of: a) generating a token based on a data

having the lowest frequency of generation among the voice data outputted from a vocoder of the wireless communication terminal; b) at a transmission terminal receiving a request for a secure communication from a user and transmitting the token to a reception terminal; and c) at the transmission terminal entering into a secure communication mode based on an acknowledge token transmitted from the reception terminal, and performing secure communication with the reception terminal.

Brief Description of the Drawings

The above and other objects and features of the present invention will become apparent from the following description of the preferred embodiments given in conjunction with the accompanying drawings, in which:

Fig. 1 is a block diagram showing a transmission terminal and a reception terminal of a wireless communication system in accordance with an embodiment of the present invention;

Fig. 2A is a flow chart describing a transmission terminal entering into a secure communication mode in accordance with an embodiment of the present invention; and

Fig. 2B is a flow chart illustrating a reception terminal entering into a secure communication mode in accordance with an embodiment of the present invention.

Detailed Description of the Invention

Other objects and aspects of the invention will become apparent from the following description of the embodiments with reference to the accompanying drawings, which is set forth hereinafter. Here, the same reference numeral is given to the same constituents, although they appear in different drawings. Also, if further detailed description on the related prior art is considered to blur the point of the present invention, it will be omitted.

Fig. 1 is a block diagram showing a transmission terminal and a reception terminal in a wireless communication system in accordance with an embodiment of the present invention. As shown in the drawing, the transmission terminal of the wireless communication system includes a microphone 101, a vocoder 103, a voice encryption unit 105, a channel encoding unit 107 and a spread/modulation unit 109. The reception terminal includes a speaker 111, a vocoder 113, a voice decryption unit 115, a channel decoding unit 117 and a dispreading/demodulation unit 119.

A voice signal of a user which is inputted to the microphone 101 of the transmission terminal goes into the vocoder 103 and is outputted in the form of 20ms-based voice packet data. In accordance with the present invention, when the transmission terminal, i.e., a calling part, begins secure communication, a token for secure communication is generated in the voice encryption unit 105. The token is transmitted

through a channel reserved for transmitting the 20ms-based voice packet data. In short, if the user on the calling part attempts secured voice communication, the voice encryption unit 105 transmits the token to the reception terminal, i.e., a called part, through the voice channel. This way, secured voice communication can be achieved. The data format of the token is the same as that of the voice packet data. Therefore, the secured voice communication can be performed without setting the communication system additionally.

Meanwhile, since the voice data outputted from the vocoder 103 is composed of random data according to each voice signal, the token data should be able to be distinguished from the voice packet data. If the token data is not distinguished from the voice packet data, the reception terminal cannot tell whether the signal it received from the transmission terminal is a token data or voice packet data.

To make the token data distinguished from the voice packet data, data having the lowest frequency of generation are combined in an arbitrary length among the voice data outputted from the vocoder 103 and used as a header of the token. In short, among the voice data outputted from the vocoder 103, a data formed in a predetermined length, e.g., two bytes, and having the lowest generation frequency for a predetermined time, e.g., three hours, is stored as a header of the token (which is referred to as 'a token header') in the transmission and reception terminals. The first two bytes of the voice packet data, which is outputted from the vocoder 103,

are stored for a predetermined time, and then two-byte data having the lowest frequency among the values of 0x0000 ~ 0xFFFF are used as a token header.

To make much lower the probability that the token data is overlapped with the voice packet data, a data combination having the lowest generation frequency among the voice data which is outputted from the vocoder 103 and has more than two bytes, e.g., in case of a 8Kbps EVRC vocoder 103, up to 22 bytes, can be used as a token header.

Desirably, the length of the token should be shorter than the maximum output length of the vocoder 103. If the token header is shorter than the maximum output data of the vocoder 103, the other portion of the token can be transmitted as a key value to be used in an encryption algorithm. Generally, the output data of the vocoder 103 have various lengths, such as full, half, quarter and eighth rates. However, in accordance with the present invention, it is desirable to set the length of the output data at a full rate during generation of the token. This is because the maximum output length of the vocoder 103 can be secured and the length of a token header can have a wider range of selection.

The longer the maximum output data of the vocoder 103 is, the longer the token becomes. Therefore, information other than the token header can be transmitted along the token data. For example, in a data encryption standard exclusive-ORed (DESX) technology, master and session keys are used to perform secured voice communication. The same master key is used for

both transmission and reception terminals, and the session key has an arbitrary value that is generated by using the master key. In accordance with the present invention, if a session key generated in the transmission terminal is included in the token as information other than the token header, the reception terminal compares the session key transmitted from the transmission terminal with the session key generated by using the master key included in the reception terminal (to see if the keys are matched), and determines whether to enter into the secure communication mode or not.

The voice decryption unit 115 of the reception terminal determines if the data transmitted from the transmission terminal are token data or not. Here, the voice encryption unit 105 of the transmission terminal transmits the same token data repeatedly a predetermined times (for example, 240 20ms-unit frames are transmitted repeatedly for a 4.8 seconds), and if the reception terminal receives the same data considered to be token data including the token header, which is described above, repeatedly a predetermined times (for example, the identical data of a 20ms-unit frame is received three times), it concludes that the transmission terminal has attempted the secured voice communication. Accordingly, the reception terminal generates an acknowledge token and transmits the acknowledge token to the transmission terminal.

The acknowledge token is generated and transmitted in the same method as the token in the transmission terminal. At this time, the acknowledge token header is the same as or

different from the token header. After the acknowledge token is transmitted, the transmission and reception terminals enter into the secure communication mode and perform secured voice communication. Here, the above mentioned process of determining if keys are matched should be understood to be included in the process of determining if the transmission terminal is attempting secured voice communication.

Fig. 2A is a flow chart describing a transmission terminal entering into the secure communication mode, and Fig. 2B is a flow chart illustrating a reception terminal entering into the secure communication mode in accordance with an embodiment of the present invention.

At step S301, the transmission terminal is at a normal communication mode. Then, at step S303, it determines if a request for attempting secured voice communication is inputted by a user. If a request for attempting secured voice communication is inputted by a user, at step S305, the voice encryption unit 105 generates a token data based on a pre-stored token header and transmits it to the reception terminal, which is also described above.

Here, the voice encryption unit 105 transmits the same token data repeatedly a predetermined times (for example, 240 20ms-unit frames are transmitted repeatedly for 4.8 seconds), and if the reception terminal receives the same data repeatedly a predetermined times (for example, the identical data of a 20ms-unit frame are received three times), it recognizes that the transmission terminal has attempted

secured voice communication. The transmission terminal sets up the temporal length of the token data, it has transmitted repeatedly (for example, in case of 240 20ms-unit frames are transmitted repeatedly, 4.8 seconds) as a token transmission time for transmitting the token. Then, at steps S307 and S309, it determines whether an acknowledge token is transmitted from the reception terminal during the token transmission time, which is set up from the beginning point of token data transmission.

If the acknowledge token is not received during the token transmission time, the transmission terminal continues to generate the token data and transmit them to the reception terminal. While checking out whether the acknowledge token is received continuously, if the token transmission time is out, the logic goes to the step S301 and the transmission terminal maintains the normal communication mode. If the transmission terminal receives an acknowledge token, at step S311, it enters into the secure communication mode, because the transmission of the acknowledge token means that the reception terminal has entered into the secure communication mode.

Meanwhile, at step S313, the reception terminal remains in a normal communication mode. Then, at step S315, it determines whether token data for secured voice communication are transmitted from the transmission terminal. If a token data for secured voice communication is transmitted from the transmission terminal, at step S317, the voice decryption unit 115 generates an acknowledge token in response to the token

for secured voice communication and transmits the acknowledge token to the transmission terminal. The acknowledge token data is generated based on a pre-stored acknowledge token header, and transmitted to the transmission terminal.

Here, at step S319, the voice decryption unit 115 transmits the same acknowledge token data repeatedly a predetermined times. At steps S307 and S309, the transmission terminal sets up the temporal length of the token data it transmitted repeatedly at step S305, for example, in case where 240 20ms-unit frames are transmitted repeatedly, the temporal length is 4.8 seconds, as a token transmission time. Then, at steps S307 and S309, it determines whether an acknowledge token is transmitted from the reception terminal during the token transmission time, which is set up from the beginning time of the token data transmission. If an acknowledge token is received, at step S311, the transmission terminal enters into the secure communication mode, just as described before. After the step S319, the reception terminal enters into the secure communication mode from the normal communication mode.

The method of the present invention can be embodied as a program and stored in a computer-readable recording medium, such as CD-ROMs, RAMs, ROMs, floppy disks, hard disks, optical-magnetic disks and the like.

The method of the present invention eliminates the need of transmitting additional messages or signals for entering into the secure communication mode by analyzing the voice

signals of the transmission and reception terminals and using the data having the lowest frequency of use as a token data. Since no additional messages are needed, secured voice communication can be performed without a change in the conventional mobile communication system establishment.

While the present invention has been described with respect to certain preferred embodiments, it will be apparent to those skilled in the art that various changes and modifications may be made without departing from the scope of the invention as defined in the following claims.